

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- x
UNITED STATES OF AMERICA,

-against-

S7 and S10 98-cr-1023 (LAK)

KHALID AL FAWWAZ and ANAS AL LIBY,

Defendants.
----- x

ORDER

LEWIS A. KAPLAN, *District Judge*.

The Memorandum and Order with Respect to the Government's Motion Pursuant to Section 6 of CIPA, dated December 11, 2014, was filed under seal with the Classified Information Security Officer ("CISO"). The Court has been advised by the CISO that the attached copy of that Memorandum and Order, reviewed and redacted by the appropriate authorities in accordance with the Classified Information Procedures Act, now may be filed on the public record. Accordingly, the Clerk shall file the attached copy in place of the half sheet [DI 1801].

SO ORDERED.

Dated: February 9, 2015

A handwritten signature in black ink, appearing to read "L. Kaplan".

Lewis A. Kaplan
United States District Judge

SECRET//NOFORN

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FILED WITH THE
CLASSIFIED INFORMATION
SECURITY OFFICER

-----x
UNITED STATES OF AMERICA

-against-

S7 and S10 98-cr-1023 (LAK)

Filed with Classified
Information Security Officer

KHALID AL FAWWAZ and ANAS AL LIBY,

CISO

Defendants.

Date

1/12/14

-----x
**MEMORANDUM AND ORDER WITH RESPECT TO THE GOVERNMENT'S
MOTION PURSUANT TO SECTION 6 OF CIPA**

LEWIS A. KAPLAN, *District Judge.*

The Classified Information Procedures Act ("CIPA") "establishes procedures for handling classified information in criminal cases."¹ Section 6 of CIPA provides that the "United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding."² The government may request such a hearing in response to a defense notification under Section 5 of its intention to disclose classified information³ or "in any other situation where the Government wished to resolve issues concerning classified information before trial."⁴ Sections 6(a) and 6(c) of CIPA provide that such a hearing must be held *in camera* if the

1

United States v. Aref, 533 F.3d 72, 78 (2d Cir. 2008).

CIPA defines "classified information" as "information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security." 18 U.S.C. App. 3 § 1(a).

2

Id. § 6(a).

3

See id. § 5(a).

4

H.R. CONF. REP. NO. 96-1436, at 12 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4307, 4310.

SECRET//NOFORN

2

Attorney General certifies to the Court that a public proceeding may result in the disclosure of classified information.⁵

On September 29, 2014, the government moved for an *in camera* hearing pursuant to Section 6 of CIPA to address the use, relevance, and admissibility of classified information it seeks to use in its case-in-chief at trial. Specifically, the government wishes to introduce involving al Fawwaz and other alleged co-conspirators,⁶ and (2) extracted from the forensic image of a computer. The Court conducted an *in camera* hearing on November 12, 2014, and has reviewed carefully the materials in question.⁷

I.

Prior to filing the indictment in this case, the government learned that another component of the U.S. government had come into possession several alleged al Qaeda members, including Khalid al Fawwaz⁸ The prosecution requested that the component of the U.S. government preserve and subsequently identified evidence relevant to the charges in this case.⁹ It now seeks to introduce

5

18 U.S.C. App. 3 § 6(a), (c).

6

Hr'g Tr. (Nov. 12, 2014) (under seal), at 5 ("I do want to note at the outset, Judge, that our motion identified There is actually of this proceeding here.").

7

The government submitted the declaration of John P. Carlin, the Assistant Attorney General in charge of the National Security Division of the United States Department of Justice, affirming that a public hearing on any part of the matter may result in the disclosure of classified information. Mr. Carlin is designated by the Attorney General for the purpose of making this certification. 18 U.S.C. App. 3 § 14.

8

Gov't CIPA Section 6 Mot. (Sept. 29, 2014), at 6.

9

Id.

SECRET//NOFORN

3

A. *Authenticity*

The parties have stipulated that the _____ are authentic within the meaning of Federal Rule of Evidence 901 in that they constitute _____

_____ as reflected by the Stipulated Protective Order with Respect to the _____ Pursuant to CIPA § 6.

“Authentication of course merely renders _____ admissible, leaving the issue of their ultimate reliability to the jury.”¹⁰ Defense counsel “remain[] free to challenge the reliability of the evidence, to minimize its importance, or to argue alternative interpretations of its meaning, but these and similar other challenges go to the *weight* of the evidence – not to its *admissibility*.”¹¹

Moreover, the government intends at trial to identify the speakers involved through cooperator and/or agent testimony, offer evidence corroborating the accuracy _____ and establish the admissibility of the contents _____ as non-hearsay statements of a party opponent or of a co-conspirator in furtherance of the conspiracy.¹² The admissibility _____ under Rule 801(d)(2)(E), to the extent offered to prove their truth, remains subject to proof at trial that such a conspiracy existed, that the defendant and the declarant participated in the conspiracy, and that the statements were made during the course of and in furtherance of that conspiracy.¹³ Accordingly, any evidentiary objections as to the admissibility of specific _____ need not be dealt with at this time.¹⁴

¹⁰

United States v. Tropeano, 252 F.3d 653, 661 (2d Cir. 2001).

¹¹

United States v. Tin Yat Chin, 371 F.3d 31, 38 (2d Cir. 2004).

¹²

Hr’g Tr. (Nov. 12, 2014) (under seal), at 11 (“Judge . . . we are simply seeking a ruling regarding authenticity. We will prove up the contents of the statements, whether _____ involved, but what we are looking for is a ruling from this Court are, in fact, _____ in question.”); *see also* Gov’t CIPA Section 6 Mot., at 14-15, 20.

¹³

See United States v. Pudilla, 203 F.3d 156, 161 (2d Cir. 2000).

¹⁴

See Hr’g Tr. (Nov. 12, 2014) (under seal), at 19.

SECRET//NOFORN

4

B. Protection of

The government seeks also to prevent

“The government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation
disclosing
“could be expected to cause exceptionally grave damage to the national security” and is not “relevant and helpful” to the preparation of the defense.¹⁵ That remains true. Indeed, nothing about the
non, impeaches any evidence of guilt, or makes more or less probable any fact at issue in establishing any defense to the charges.”¹⁷ Such information properly was withheld from discovery pursuant to Section 4 of CIPA and Federal Rule of Criminal Procedure 16(d)(1).

Accordingly, to prevent the public disclosure of this information, the parties shall not examine any witness, introduce any evidence, or make any arguments with respect to those topics enumerated in the Stipulated Protective Order with Respect to the
Pursuant to CIPA § 6.

counsel reference other
written approval.

Nor shall defense
for which they have not obtained the Court’s

II. Computer Materials

In November 1998,
¹⁸

dispatched a technical officer to create a forensic

¹⁵

CIA v. Sims, 471 U.S. 159, 175 (1985) (internal quotation marks omitted).

¹⁶

Prot. Order with Respect to Certain Disc. (Sept. 24, 2013) [DI 1318] ¶¶ 2-3.

¹⁷

United States v. Yunis, 867 F.2d 617, 624 (D.C. Cir. 1989).

¹⁸

Computer Decl. (Sept. 29, 2014) (submitted *ex parte* and *in camera*) [Gov’t CIPA Section 6 Mot., Ex. E] ¶¶ 14-16.

SECRET//NOFORN

5

image of the computer and to restore contents of the computer that appeared to have been deleted by the user.¹⁹ The government seeks to introduce certain documents and reports obtained from the forensic image of the computer (the "Computer Materials") in its case-in-chief at trial, subject to protections against disclosure of the source of acquisition.

A. Authenticity

The government requests a pretrial determination that the Computer Materials are authentic pursuant to Federal Rule of Evidence 901(a). The defense contends that such a finding is not appropriate because the government cannot establish a chain of custody prior imaging of the computer.

Rule 901(a) requires the government to submit "evidence sufficient to support a finding that the matter in question is what its proponent claims." Rule 901's requirements are satisfied "if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification."²⁰ It "does not erect a particularly high hurdle," and may be satisfied by "circumstantial evidence."²¹ Moreover, "[b]reaks in the chain of custody do not bear upon the admissibility of evidence, only the weight of the evidence."²²

After considerable discussion at the *in camera* hearing, the parties stipulated to the following:

"[A]fter obtaining the computer forensic image of its contents without otherwise affecting the contents of the computer dispatched a technical officer, to create a forensic image of the computer while it remained Throughout the imaging process, The forensic image of the computer then was transported to the United States for further processing. An initial review

¹⁹

Id. ¶¶ 15-16.

²⁰

United States v. Ruggiero, 928 F.2d 1289, 1303 (2d Cir. 1991) (internal quotation marks omitted).

²¹

United States v. Dhinsa, 243 F.3d 635, 658 (2d Cir. 2001) (internal quotation marks omitted).

²²

United States v. Morrison, 153 F.3d 34, 57 (2d Cir. 1998).

SECRET//NOFORN

6

of the forensic image revealed that certain of the computer's contents had been deleted by its user using multiple technical experts and then classified and unavailable methods, restored the deleted contents of the forensic image. . . . [W]hile in 1998 the methods used were not available, they have subsequently become available and are commercially available. . . . [A]fter the deleted files were restored[,] the documents and images contained on the forensic image were printed out on paper."²³

Accordingly, the Court finds that the Computer Materials are authentic within the meaning of Rule 901. The defense nonetheless may "develop testimony related to . . . alleged tampering" of the computer before it came into possession of the U.S. government and/or argue that issue to the jury because it is an issue of the "weight rather than admissibility" of the evidence.²⁴ That may prove to be a potent issue for the government's case-in-chief, but it is not a bar to authentication.

B. Admissibility

The government requests also a pretrial determination that the Computer Materials are admissible at trial.

First, the materials are not barred by the hearsay rule. "Out-of-court statements constitute hearsay only when offered in evidence to prove the truth of the matter asserted."²⁵ It is not hearsay where a party intends to prove that a prior statement was made and not to prove the truth of that statement. Thus, "[s]tatements offered as evidence of commands or threats or rules directed to the witness, rather than for the truth of the matter asserted therein, are not hearsay."²⁶ Moreover, where "the statement is offered as circumstantial evidence of [a defendant's] state of mind, it does not fall within the definition given by Rule 801(c)[] because it was not offered to prove the truth of the matter asserted."²⁷

²³

Hr'g Tr. (Nov. 12, 2014), at 48.

²⁴

United States v. Sovie, 122 F.3d 122, 127-28 (2d Cir. 1997).

²⁵

Anderson v. United States, 417 U.S. 211, 219 (1974).

²⁶

United States v. Bellomo, 176 F.3d 580, 586 (2d Cir. 1999).

²⁷

United States v. Salameh, 152 F.3d 88, 112 (2d Cir. 1998) (alteration in original) (internal quotation marks omitted).

SECRET//NOFORN

7

Here, many of the documents that the government seeks to introduce constitute directives, threats, or statements of intent, and will be used only to prove that such statements were made, not to prove the truth of the matters asserted. To the extent that portions of the Computer Materials contain assertions requiring the government to offer them for the truth of the matters asserted therein, the government may seek to admit them as non-hearsay statements of a co-conspirator.²⁸ The admissibility of the Computer Materials on that basis remains subject to proof that such a conspiracy existed, that the defendant and the declarant participated in the conspiracy, and that the statement was made during the course of and in furtherance of that conspiracy.²⁹

Second, the probative value of the Computer Materials is not substantially outweighed by the danger of unfair prejudice to the defendants. Relevant evidence may be excluded under Rule 403 if “its probative value is substantially outweighed by a danger of . . . unfair prejudice, confusing the issues, [or] misleading the jury.”³⁰ The Advisory Committee Notes state that unfair prejudice is “an undue tendency to suggest decision on an improper basis, commonly, though not necessarily, an emotional one.”³¹

The Computer Materials provide background information regarding the alleged conspiracy and its targeting of U.S. interests. Moreover, the Computer Materials are probative of the existence of a conspiracy and of its members because the same (or similar) documents are linked to defendants and other alleged co-conspirators.

Al Fawwaz contends, however, that it would be unfairly prejudicial to admit the Computer Materials because the jury improperly will infer that they represent a collection of al Qaeda documents.³² The government argues that there is no danger of unfair prejudice because the defense may argue to the jury that the computer was manufactured out of whole cloth.³³

Here, there is no danger of improper reasoning. The defense undoubtedly will argue that no evidence has been introduced as to the origins of the computer before it came into

²⁸

See FED. R. EVID. 801(d)(2)(E).

²⁹

See Padilla, 203 F.3d at 161.

³⁰

FED. R. EVID. 403.

³¹

FED. R. EVID. 403 advisory committee’s note.

³²

Hr’g Tr. (Nov. 12, 2014), at 30.

³³

Id. at 37-39.

SECRET//NOFORN

8

possession of the U.S. government and that the contents may have been entirely fabricated or manufactured. It is the government that will need to tie these documents to the defendants in order to convince the jury that they are what they purport to be and that they are reliable. The jury may choose to accept or reject the reliability of such evidence, but that goes to the weight the jury affords them, not their admissibility. Indeed, “[e]vidence is not unfairly prejudicial because it tends to prove guilt, but because it tends to encourage the jury to find guilt from improper reasoning.”³⁴ Thus, there is no reason to believe that the jury is likely to draw an improper conclusion from the Computer Materials.

Third, admission of the Computer Materials would not violate the Confrontation Clause. *Crawford v. Washington*³⁵ announced a *per se* bar on the admission of testimonial out-of-court statements unless the declarant is unavailable and the defendant has had a prior opportunity to cross-examine the declarant regarding the statement.³⁶ The government correctly argues, however, that *Crawford* does not apply because the government will not introduce any testimonial statement about where or from whom the computer was obtained prior to the time it came into the U.S. government’s possession.³⁷ The defense remains free to “undercut the weight that the jury should give” to the Computer Materials because no evidence will be presented about where the computer came from or from whom it was taken prior to the time it came into the United States’ possession.³⁸

The Court concludes that the Computer Materials are admissible to the extent they are offered for purposes other than their truth. To the extent they are offered to prove their truth, the government will be obliged to establish that they are admissible under Rule 801(d)(2)(E) or a hearsay exception.

³⁴

United States v. Looking Cloud, 419 F.3d 781, 785 (8th Cir. 2005).

³⁵

541 U.S. 36 (2004).

³⁶

Id. at 59, 68; *see also United States v. Stewart*, 433 F.3d 273, 290 (2d Cir. 2006) (“*Crawford* . . . announced a *per se* bar on the admission of a class of out-of-court statements, denominated ‘testimonial,’ against an accused who had no prior opportunity to cross-examine the declarant.”).

³⁷

Hr’g Tr. (Nov. 12, 2014), at 41.

³⁸

Id.

SECRET//NOFORN

9

C. *Protection of the Source of Acquisition*

The government seeks also to prevent disclosure of the source from which the Computer Materials were obtained, pursuant to Section 6(c) of CIPA. That provision permits the government to seek an order to substitute “a summary of the specific classified information.”³⁹ The Court must authorize substitution if “the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information.”⁴⁰

The government requests that the Court authorize it to substitute protect the national security interests at issue.⁴¹ The Court finds that the requested substitutions offer the defendants substantially the same ability to make their defense. It is the government that has chosen to forego evidence in its case-in-chief that,

⁴² Defendants may argue that the jury should not give any weight to the Computer Materials because no evidence was offered regarding who owned the computer or what was done with it before it was forensically imaged. In short, the Court finds that the defense will not be prejudiced by the substitutions in any way.

Moreover, the government will stipulate that the foreign country from which the computer was recovered is not Sudan, the United Kingdom, Kenya, Yemen, Pakistan, or Afghanistan, and that the computer was not recovered from al Fawwaz or al Liby or their residences or offices.⁴³ These stipulations protect against any possibility that the jury would draw any improper inference from the lack of specificity regarding the origins of the Computer Materials.

39

18 U.S.C. App. 3 § 6(c).

40

Id.

41

The government requests the following specific substitutions: (1) “In or about November 1998, an employee of the United States Government forensically imaged a computer (the ‘Computer’) while stationed in a foreign country (the ‘Foreign Country’);” and (2) “After receiving the Computer, arrangements were made for an employee of the United States to travel to the Foreign Country to make a forensic image of the Computer.” Gov’t CIPA Section 6 Mot., at 29.

42

Id. at 31.

43

Id. at 32.

SECRET//NOFORN


10

Finally, to prevent against the public disclosure of this classified information important to national security, the parties shall not examine any witness, introduce any evidence, or make any arguments with respect to:

As classified materials are involved here, the motion pursuant to Section 6 of CIPA and all papers submitted in connection therewith and the transcript from the *in camera* hearing with this Court shall be filed under seal with and maintained by the Court's Classified Information Security Officer designated in accordance with CIPA and the *Security Procedures Established Pursuant to Pub. L. No. 96-456* by the Chief Justice of the United States.

SO ORDERED.

Dated: December 11, 2014



Lewis A. Kaplan
United States District Judge

SECRET//NOFORN